SECTION XV. COMSEC EMERGENCY ACTION PROCEDURES

103. Emergency Protection Planning. All facilities which hold classified or CCI COMSEC material must maintain a current, written emergency plan for the protection of such material during emergencies. For locations in CONUS, planning need consider only natural disasters (such as fire, flood, tornado, and earthquake). For locations outside of CONUS, planning must consider both natural disasters and hostile actions (such as enemy attack, mob action, civil uprising). For natural disasters, planning should be directed toward maintaining security control over the material until order is restored. By contrast, planning for hostile actions must concentrate on actions to safely evacuate or securely destroy the COMSEC material. Normal operating routines must be structured so as to minimize the number and complexity of actions which must be taken during emergencies to protect COMSEC material. For example:

a. Only the minimum amount of COMSEC material will be held at any time; i.e., routine destruction should be conducted frequently and excess COMSEC material disposed of in accordance with the disposition instructions obtained from the cognizant contracting officer.

b. COMSEC material should be stored in ways which will facilitate emergency evacuation or destruction.

104. Preparedness Planning for Disasters. Planning for disasters must provide for:

a. Fire reporting and initial fire fighting by assigned personnel.

b. Assignment of on-the-scene responsibility for ensuring protection of the COMSEC material held.

c. Securing or removal of classified COMSEC material and evacuation of the area(s).

d. Protection of material when admission of outside fire fighters into the secure area(s) is necessary.

e. Assessment and reporting of probable exposure of classified COMSEC material to unauthorized persons during the emergency.

f. Post-emergency inventory of classified and CCI COMSEC material and the reporting of any losses or unauthorized exposures to appropriate authority.

105. Preparedness Planning for Hostile Actions. Planning for hostile actions must take into account the possible types of situations which may occur; e.g., an ordered withdrawal over a specified period of time, a hostile environment situation where destruction must be carried out in a discrete manner to avoid triggering hostile actions, or fully hostile imminent overrun situations. Such planning must provided for:

a. Assessing the threat of occurrence of various types of hostile actions at the particular activity and the threat which these potential emergencies pose to the COMSEC material held.

b. Availability and adequacy of physical security protection capabilities; e.g., perimeter controls, guard forces, and physical defenses at the individual buildings and other locations in which COMSEC material is held.

c. Facilities for effecting emergency evacuation of COMSEC material under emergency conditions, including an assessment of the probable risks associated with evacuation. 1/

d. Facilities and procedures for effective secure emergency destruction of COMSEC material held, including adequate supplies of destruction devices, availability of electrical power, secure nearby storage facilities, adequately protected destruction areas, personnel assignments, and responsibilities for implementing emergency destruction.

e. Precautionary destruction of COMSEC material, particularly maintenance manuals and keying material, which is not operationally required to ensure continuity of operations during the emergency. In a deteriorating situation all “full” maintenance manuals (i.e. , those containing cryptographic logic information) which are not absolutely essential to continued mission accomplishment should be destroyed. When there is insufficient time under emergency conditions to completely destroy such manuals, every reasonable effort must be made to remove and destroy their sensitive pages (i.e., those containing cryptographic logic). Sensitive pages in U.S.-produced KAMs are listed on fold-out Lists of Effective Pages at the rear of other textual portions and, in addition, some KAMs further identify their sensitive pages by means of gray or black diagonal or rectangular markings at the upper portion of the binding edge.

(1) To prepare for possible emergency destruction sensitive pages from COMSEC maintenance manuals in areas or situations where capture by hostile forces is possible, the following is suggested:

(a) Apply distinctive markings (e.g., red stripes) to the binder edge and covers of all KAMs containing identified sensitive pages.

(b) Remove the screw posts or binder rings, or open the multiring binder, whichever is applicable.

(c) Remove each sensitive page from the KAM and cut off the upper left-hand corner of the page so that the first binder hole is removed. Care must be taken not to delete any text or diagram.

1/ Except under extraordinary conditions (e.g., an urgent need to restore secure communications after relocation), COMSEC keying material should be destroyed rather than evacuated.

(d) Reassemble the document and conduct a page check.

(2) Should it become necessary to implement emergency destruction, the sensitive KAM pages may be removed as follows:

(a) Remove the screw posts or binder rings, or open the multiring binder and remove all pages from the KAM.

(b) Insert a thin metal rod (e.g., wire or screwdriver) through the remaining top left-hand hole of the document.

(c) Grasp the rod in both hands and shake the document vigorously; the sensitive pages should fall out freely.

f. External communications during emergency situations should be limited to contact with a single remote point. This point will act as a distribution center for outgoing message traffic, and as a filter for incoming queries and guidance, thus relieving site personnel and facilities from multiple actions during emergency situations. When there is warning of hostile intent and physical security protection is inadequate to prevent overrun of the facility, secure communications should be discontinued in time to allow for thorough destruction all classified and CCI COMSEC material, including classified and CCI elements of COMSEC equipment.

106. Preparing the Emergency Plan. Preparation of the emergency plan is the responsibility of the FSO. If the plan calls for destroying the COMSEC material, all destruction material, devices, and facilities must be readily available and in good working order. The plan must be realistic; it must be workable, and it must accomplish the goals for which it is prepared. Factors which will contribute to this are:

a. All duties under the plan must be clearly and concisely described.

b. All authorized personnel at the facility should be aware of the existence of the plan. Each individual who has duties assigned under the plan should receive detailed instructions on how to carry out these duties when the plan becomes effective. All personnel should be familiar with all duties so that changes in assignment may be made, if necessary. This may be accomplished by periodically rotating the emergency duties of all personnel.

c. Training exercise should be conducted periodically (quarterly exercises are recommended) to ensure that everyone, especially newly assigned personnel who might have to take part in an actual emergency, will be able to carry out their duties. If necessary, the plan should be changed based on the experience of the training exercises.

d. The three options available in a hostile-action emergency are securing the material, removing it from the scene of the emergency, or destroying it. Planners must consider which of these may be applicable to their facilities, either singly or in a combination. Which one to choose in various situations should be clearly stated in the plan. For example, if it appears that a civil uprising is to be short lived, and the COMSEC facility is to be only temporarily abandoned, the actions to take could be:

(1) Ensure that all superseded keying material has been destroyed.

(2) Gather up the current and future keying material and take it along.

(3) Remove all classified and CCI elements from crypto-equipment and lock them, along with other classified COMSEC material, in approved storage containers.

(4) Secure the facility door(s), and leave.

(5) Upon return, conduct a careful and complete inventory.

Or, if it appears that the facility is likely to be overrun, the emergency destruction plan should be put into effect.

107. Emergency Destruction Priorities. Three broad categories of COMSEC material which may require destruction in hostile-action emergencies are keying material; other COMSEC aids (e.g., maintenance manuals, operating instructions, and general doctrinal publications); and equipment. Depending upon the availability of sufficient personnel and destruction facilities, the priorities set forth under subparagraphs a. or b., below, must be followed.

a. Destruction Priorities within Categories COMSEC Material. When sufficient personnel and destruction facilities are available, different individuals should be made responsible for destroying the material in each category, by means of separate destruction facilities, as set forth in the following subparagraphs:

(1) Keying Material. Emergency destruction priorities for keying material are as follows:

(a) Superseded keying material designated CRYPTO.

(b) Currently effective keying material designated CRYPTO (to include zeroization of keying variables stored electrically in crypto-equipment and fill-devices).

(c) Card Reader Insert Boards (CRIBS).

(d) Future editions of TOP SECRET keying material designated CRYPTO .

(e) Future editions of SECRET and CONFIDENTIAL keying material designated CRYPTO.

(f) Training, maintenance, and sample key.

(2) Other COMSEC Aids. Emergency destruction priorities for classified COMSEC Aids other than keying material are as follows:

(a) Complete cryptomaintenance manuals or sensitive pages, thereof.

(b) Status documents showing the effective dates for COMSEC keying material.

(c) Keying material holder lists and directories.

(d) Remaining classified pages of cryptomaintenance manuals.

(e) Classified cryptographic and noncryptographic operational general publications (KAGs and NAGs).

(f) Cryptographic Operating Instructions.

(g) Remaining classified COMSEC documents

(h) National, department, agency, and service general doctrinal guidance publications.

(3) COMSEC Equipment. Reasonable efforts should be made under deteriorating situations to evacuate COMSEC equipment. In an actual emergency, the immediate goal is to render COMSEC equipment unusable and irreparable. 2/ When there is warning of hostile intent, secure communications should be discontinued in advance to allow for thorough destruction of COMSEC equipment. Emergency destruction priorities for COMSEC equipment are as follows:

(a) Zeroize the equipment if the keying element (e.g., key card, permuter plug) cannot be physically withdrawn.

(b) Remove and destroy removable classified and CCI elements (e.g., printed-circuit boards).

(c) Destroy remaining classified and CCI elements.

NOTE : Hulks of equipments and unclassified elements not marked CCI, need not be destroyed. Maintenance manuals for COMSEC equipment contain component listings which identify classified and CCI elements.

b. Destruction Priorities for Combined Categories of COMSEC Material. When personnel and/or destruction facilities are limited, the three categories of COMSEC material will be combined, and destruction will be carried out in accordance with the following priority listing:

(1) All keying material_ designated CRYPTO, in the following order: superseded key, currently effective key, future key.

(2) Sensitive pages from classified maintenance manuals, or the entire manual (if sensitive pages are not separately identified).

(3) Classified and CCI elements of classified and CCI COMSEC equipment.

2/ Although it is desirable to destroy jeopardized crypto-equipment so thoroughly that logic reconstruction is impossible, this cannot be guaranteed in most field environments.

(4) Any remaining classified COMSEC or related material.

NOTE : Hulks of equipment, unclassified elements not marked CCI, and unclassified portions of maintenance manuals, operating instructions, etc., need not be destroyed.

108. Emergency Destruction Tools. Basic hand tools should be readily available for emergency destruction of COMSEC equipment at all facilities holding such equipment. These tools will be useful, and in some cases required, for removing classified and CCI elements from equipment, for removing certain components from classified and CCI elements prior to disintegrator destruction and, in worst-case situations, to actually accomplish destruction. The following is a list of suggested tools which should be kept in a designated area reserved exclusively for emergency destruction of COMSEC equipment:

- Hammer, 3-lb, ball or cross peen
- Cold chisel, 5-3/4-inches long, l/2-inch wide tip
- Stubby screwdriver, l-inch blade, 7/32-inch wide tip
- Screwdriver, l-l/2-inch blade, 5/32-inch wide tip
- Screwdriver, 6-inch blade, 5/16-inch wide tip
- Phillips screwdriver, number O
- Phillips screwdriver, number 2
- Wrench, 5/16, box- and open-end combination
- Pliers, 5-inch, diagonal cutting
- Pliers, heavy duty, linemans
- Crowbar
- Fire ax or sledge hammer

In addition to the above hand tools, facilities which maintain an incinerator for emergency destruction should also have tongs and asbestos gloves readily available.

109. Emergency Destruction Methods. Any of the methods approved for routine destruction of classified COMSEC material may be used for emergency destruction. Additionally, incendiary destruction devices may be available for emergency destruction at certain locations outside of CONUS. Information concerning these devices is contained in NTISSI No. 4004, “Routine Destruction and Emergency Protection of COMSEC Material.”

110. Reporting Emergency Destruction. Accurate information relative to the extent of an emergency destruction is absolutely essential to the effective

evaluation of the COMSEC impact of the occurrence, and is second in importance only to the conduct of thorough destruction. Reports must be submitted by the most expeditious means available and shall clearly indicate the material destroyed, the method(s) of destruction, and the extent of destruction. The report must also identify any items which were not throughly destroyed and which may be presumed to be compromised. In such cases, an insecurity report must be submitted as prescribed in Section XVI.

111. Review of Emergency Action Procedures. COMSEC emergency procedures developed under these guidelines will be made available for review upon the request of NSA.